AO 106 (Rev. 04/10) Application for a Search Warrant



# UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of
*(Briefly describe the property to be searched or identify the person by name and address)*

The subject premises of 8575 Vinup Rd, Apt. B, Lynden, Washington

Case No. MJ17-519

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

The subject premises of 8575 Vinup Rd, Apt. B, Lynden, Washington as further described in Attachment A, which is attached hereto and incorporated herein by this reference.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, which is attached hereto and incorporated herein by this reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| *Code Section* | *Offense Description* |
|---|---|
| Title 18, U.S.C. § (2252 (a)(2) | Receipt or Distribution of Child Pornography and |
| Title 18, U.S.C. § (2252(a)(4)(B) | Possession of Child Pornography |

The application is based on these facts:

See attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

*Applicant's signature*

SPECIAL AGENT TOBY LEDGERWOOD, DHS/HSI
*Printed name and title*

Sworn to before me pursuant to CrimRule 4.1.

Date: 12-14-17

*Judge's signature*

City and state: SEATTLE, WASHINGTON

PAULA L. MCCANDLIS, U.S. MAGISTRATE JUDGE
*Printed name and title*

2017R01278

# ATTACHMENT A

## Description of Property to be Searched

The physical address of the SUBJECT PREMISES is 8575 Vinup Rd, Apt B, Lynden, Washington, and is more fully described as Unit B of the two-story, multi-unit residence with brown colored siding and white trim around the windows. The numbers 8575 are affixed in black lettering on the side of the building above the fire extinguisher. The letter "B" is in black located on a white door marking "Unit B." There are windows located on either side of the door to Unit B.

The search is to include all rooms and persons within the SUBJECT PREMISES, and all garages or storage rooms, attached or detached, or other outbuildings assigned to Unit B, and any digital device(s) found therein.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

**ATTACHMENT B**

**ITEMS TO BE SEIZED**

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed), photocopies or other photographic form, and electrical, electronic, and magnetic form (such as CDs, DVDs, smart cards, thumb drives, camera memory cards, electronic notebooks, or any other storage medium), that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) which may be found at the SUBJECT PREMISES:

1. Any visual depiction of minor(s) engaged in sexually explicit conduct, in any format or media.

2. Evidence of the installation and use of P2P software, and any associated logs, saved user names and passwords, shared files, and browsing history;

3. Letters, e-mail, text messages, and other correspondence identifying persons transmitting child pornography, or evidencing the transmission of child pornography, through interstate or foreign commerce, including by mail or by computer;

4. All invoices, purchase agreements, catalogs, canceled checks, money order receipts, credit card statements or other documents pertaining to the transportation or purchasing of images of minors engaged in sexually explicit conduct;

5. Any and all address books, names, lists of names, telephone numbers, and addresses of individuals engaged in the transfer, exchange, or sale of child pornography;

6. Any non-digital recording devices and non-digital media capable of storing images and videos.

7. Digital devices and/or their components, which include, but are not limited to:

a. Any digital devices and storage device capable of being used to commit, further, or store evidence of the offense listed above;



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

b. Any digital devices used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, cameras, printers, encryption devices, and optical scanners;

c. Any magnetic, electronic, or optical storage device capable of storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or memory buffers, smart cards, PC cards, memory sticks, flashdrives, USB/thumb drives, camera memory cards, media cards, electronic notebooks, and personal digital assistants;

d. Any documentation, operating logs and reference manuals regarding the operation of the digital device or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

g. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data;

8. Evidence of who used, owned or controlled any seized digital device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, saved user names and passwords, documents, and browsing history;

9. Evidence of malware that would allow others to control any seized digital device(s) such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malware; as well as evidence of the lack of such malware;

10. Evidence of the attachment to the digital device(s) of other storage devices or similar containers for electronic evidence;

11. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from a digital device;



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

12. Evidence of times the digital device(s) was used;

13. Any other ESI from the digital device(s) necessary to understand how the digital device was used, the purpose of its use, who used it, and when.

14. Records and things evidencing the use of the IP address 73.53.83.83 (the SUBJECT IP ADDRESS) including:

a. Routers, modems, and network equipment used to connect computers to the Internet;

b. Records of Internet Protocol (IP) addresses used;

c. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

**The seizure of digital devices and/or their components as set forth herein is specifically authorized by this search warrant, not only to the extent that such digital devices constitute instrumentalities of the criminal activity described above, but also for the purpose of the conducting off-site examinations of their contents for evidence, instrumentalities, or fruits of the aforementioned crimes.**



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

# AFFIDAVIT

STATE OF WASHINGTON )
) ss
COUNTY OF KING )

I, Toby Ledgerwood, being duly sworn on oath, depose and state:

## I. INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the U.S. Department of Homeland Security, Homeland Security Investigations (HSI), assigned to the Assistant Special Agent in Charge (ASAC) Blaine, Washington, field office. I have been employed as an HSI Special Agent since 2006. Prior to this assignment, I worked as a United States Customs Inspector from 2002 to 2006. In my capacity as a Special Agent, I am responsible for conducting investigations into the numerous federal laws enforced by HSI. Since 2013, I have investigated criminal violations relating to child exploitation and child pornography, including violations pertaining to the unlawful production, importation, distribution, receipt, attempted receipt, and possession of child pornography and material involving the sexual exploitation of minors in violation of 18 U.S.C. §§ 2251, 2252(a), and 2252A(a). I am a graduate of the Federal Law Enforcement Training Center (FLETC), HSI Special Agent Training Program, and have received further specialized training in investigating child pornography and child exploitation crimes. My training included courses in law enforcement techniques, federal criminal statutes, conducting criminal investigations, and the execution of search warrants. I have observed and reviewed thousands of examples of child pornography (as defined in 18 U.S.C. § 2256(8)). I have participated in the execution of many search warrants which involved child exploitation and/or child pornography offenses and the search and seizure of computers and other digital devices. Further, I have served as the affiant on numerous search warrants and complaints relating to child exploitation investigations. I am a member of the Internet



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Crimes Against Children (ICAC) Task Force in the Western District of Washington, and work with other federal, state, and local law enforcement personnel in the investigation and prosecution of crimes involving the sexual exploitation of children. I have attended periodic seminars, meetings, and training. I attended the ICAC Undercover Investigations Training Program in Alexandria, Virginia, in June 2014 regarding child exploitation. I also attended the Crimes Against Children Conference in Dallas, Texas, in August 2014, where I received training relating to child exploitation, including training in the Ares Peer to Peer (P2P) file sharing program. In September 2015, I received training in the Emule (P2P) file sharing program. I received a Bachelor of Science degree in Criminal Justice with a minor in Sociology from the University of Missouri-St. Louis.

2. I am submitting this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the residence located at 8575 Vinup Rd, Apt B, Lynden, Washington 98264 (hereinafter the "SUBJECT PREMISES") more fully described in Attachment A, for the things specified in Attachment B to this Affidavit, for the reasons set forth below. I also seek authority to examine digital devices or other electronic storage media. The property to be searched is as follows:

a. 8575 Vinup Rd, Apt B, Lynden, Washington 98264 (the SUBJECT PREMISES);

3. The warrant would authorize a search of the SUBJECT PREMISES, any persons located within the SUBJECT PREMISES, and the seizure and forensic examination of digital devices found therein, for the purpose of identifying electronically stored data as particularly described in Attachment B, for evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography).

4. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; review of documents and records



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience.

5. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation. I have set forth only the facts that I believe are relevant to the determination of probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), will be found at the SUBJECT PREMISES.

6. Based on the discoveries I have made, as described below, I believe that someone at the SUBJECT PREMISES has used a computer to connect to the Internet, via Internet Protocol (IP) address 73.53.83.83 (hereinafter the "SUBJECT IP ADDRESS"), and distribute an image depicting child pornography. I further believe that computers and other digital devices containing evidence of child pornography will be located at the SUBJECT PREMISES.

This Affidavit is being presented electronically pursuant to Local Criminal Rule CrR 41(d)(3).

## II. DEFINITIONS

7. The following definitions apply to this Affidavit:

Internet Service Providers

a. "Internet Service Providers" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "email address," an email mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password. ISPs maintain records pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), email communications, information concerning content uploaded and/or stored on or via the ISP's servers.

Internet Protocol (IP) Addresses

b. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer connected to the Internet must be assigned an IP address so that the Internet traffic sent from, and directed to, that computer may be properly directed from its source to its destination. Most ISPs control the range of IP addresses.

## III. The CyberTip and ESP Rabbit

8. This investigation arose from a CyberTip submitted to the National Center for Missing and Exploited Children (NCMEC). NCMEC is a private non-profit organization operating under a Congressional mandate to act as the nation's law enforcement clearing house for information concerning online child sexual exploitation. In partial fulfillment of that mandate, NCMEC operates a CyberTip line, a resource for reporting online crimes against children. Electronic Service Providers (ESPs) report to NCMEC, via the CyberTip line, whenever they discover that a subscriber has violated the terms of service and/or their services have been used to transmit child pornography over the Internet.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

9. The CyberTip giving rise to this investigation came from ESP Rabbit. According to the ESP itself,

> Rabbit is about sharing your everyday. Watch your favorite shows with your friends, without being in the same room (or even the same city!). Collaborate with your coworkers when you're all on the road. Shop together for a birthday present for Mom, then sing her "happy birthday" with family far away. The possibilities are endless. Rabbit started with an idea: people sharing experiences online from wherever they are. We began with an app for Mac in February 2013. Then in August 2014, we launched a web-based version of Rabbit. In February 2-15, we were named one of the Top 10 Most Innovative Companies in Video by Fast Company. And in October 2015, we launched an app for iOS. But this is only the start: we've got big plans.

## IV. STATEMENT OF PROBABLE CAUSE

10. In December 2017, Homeland Security Investigations (HSI) Blaine, Washington received CyberTip report #25955849 from the Seattle Internet Crimes Against Children (ICAC) Task Force. The report indicated the ESP, Rabbit, reported that one of its users uploaded several images of suspected child pornography to its website. According to the CyberTip, the user was named, Lovr E, and has a screen/user name, Lovr1. The report also stated that the IP address of the device that uploaded these images of suspected child pornography was 73.53.83.83 (the SUBJECT IP ADDRESS). According to the CyberTip, that user uploaded approximately thirteen images depicting suspected child pornography between November 26, 2017, and November 27, 2017, from the SUBJECT IP ADDRESS. Before submitting the CyberTip, employee(s) of Rabbit examined each of these images of suspected of child pornography.

11. I have reviewed these images of suspected child pornography and describe each below:



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

**Filename: Lovr1_20171126_2.png**
This color image depicts a prepubescent female (hereinafter the "child victim"). The child victim is nude and laying on her back visible from her waist to her thighs. The child victim's legs are spread apart and her unclothed genital area is the focal point of the image. An orange carrot is inserted into her vagina by what appears to be an adult's hand. The child victim has no visible pubic hair and is very small in stature. The child victim appears to be approximately 5 to 6 years old.

**Filename: Lovr1_20171126_1.png**
This color image depicts a prepubescent female (hereinafter the "child victim"). The child victim is completely nude and laying on her back. She is fully visible. The child is lying on a blue blanket with black squares. The child's legs are spread apart. A hairy adult arm and hand is holding a white sex toy in front of her vagina. There appears to be a shiny lubricant around the child victim's vaginal area. The child victim's vagina is not exposed due to the sex toy being placed in front of or on it. The child victim's breasts are exposed. She has no visible pubic hair, lacks muscular and breast development and is very small in stature. The child victim appears to be approximately 5-6 years old.

12. Rabbit also provided several pages of chats from the user Lovr1. On November 26, 2017, and November 27, 2017, Lovr1 had a conversation with an unknown user discussing having an "ex's daughter" who appears to be a child named "[MV]". During this chat, Lovr1 states, "i still get my ex's daughter all the time on weekends, [S.] is always like, oh shes a cutie", "its fucking cute seeing her cuddle with her, seeing [MV] wrap her legs around [S.], its soooo hot to think about". Later in the conversation, Lovr1 states: "mmm, could use her little sisters feet to rub on [MV's] pussy:)", "mmmm god yes, i love kissing [MV's] feet", "god why is little girl pussy the hottest thing on earth", "i bet its even more amazing making a little girl cummmm", "coat that ball with KY and get [MV] and her little sister on it together!!!", "god I want [MV] to be the one to teach them aboutr their pussies !!!".

13. In addition to the above messages discussing the sexual abuse of MV, there is a series of messages in which Lovr1 recounts taking MV to a hotel over a weekend and then sends images purportedly of MV, in which MV's breasts and vagina are exposed. These images were among the images flagged (and viewed) by Rabbit and included with



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

the CyberTip. They depict a prepubescent girl between six and nine years old next to a bed, in what appears to be a hotel room.

14. A query of a publicly available database revealed the SUBJECT IP ADDRESS belonged to ISP Comcast Communications.

15. On December 06, 2017, a Department of Homeland Security (DHS) administrative summons' was submitted to Comcast requesting subscriber information for the SUBJECT IP ADDRESS during the date and time the subject image files were uploaded.

16. On December 08, 2017, Comcast provided the requested information. During the date and time the subject image files were uploaded, the SUBJECT IP ADDRESS was assigned to C.P. at the residence located at 8575 Vinup Rd, Apt B, Lynden, Washington (the SUBJECT PREMISES). Comcast revealed the IP History of the SUBJECT IP ADDRESS to have a lease grant date and time of October 20, 2017, at 19:56:45 UTC and a lease expiration of December 06, 2017, at 23:01:48 UTC. The SUBJECT IP ADDRESS is leased to C.P. with account number ending in 7795.

17. Intelligence Research Specialist/Computer Forensic Analyst (IRS/CFA) Gillie conducted records checks via a law enforcement database and found that C.P. (DOB XX/XX/1989) has been associated with the SUBJECT PREMISES since June 2017. I conducted a search via the Washington State Department of Licensing (WSDOL) and learned that C.P. has a 2007 Hyundai, registered at the SUBJECT PREMISES. WSDOL also revealed C.P. was issued a Washington State driver's license on September 12, 2017, with the SUBJECT PRIMISES listed as her address.

18. On December 8, 2017, at approximately 3:30 p.m., SA Jesse Miller conducted surveillance of the SUBJECT PREMISES and observed the following vehicle parked in the driveway: Hyundai bearing Washington State license plate BGV7348. Records checks revealed that the vehicles are registered to C.P. at the SUBJECT PREMISES.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

19. On December 11, 2017, while conducting surveillance of the SUBJECT PREMISES, SA Shaun Smith used a portable electronic device to conduct a wireless survey from the public right of way adjacent to the SUBJECT PREMISES and discovered numerous Wi-Fi enabled networks. These Wi-Fi networks were all locked. During that survey, SA Smith also detected at least one "xfinitywifi" wireless internet network in the area. Based on my training and experience, I know that Comcast deployed a series of wireless "hotspot" networks for their customers. Comcast accomplished this by providing their wireless internet customers with updated wireless routers capable of broadcasting an additional wireless network. These wireless "hotspot" networks are recognized by the connecting device as "xfinitywifi". Comcast customers can access "xfinitywifi" networks by logging in with their unique Comcast email or username and previously created password. Of particular importance is that the "xfinitywifi" networks are completely separate from the Comcast customer's private home wireless network(s). While conducting a prior investigation, an official with Comcast confirmed with me that Comcast's "xfinitywifi" wireless networks are not linked or connected to the Comcast subscriber's internet service.

20. Based on observations during surveillance, public records checks, and other investigation conducted to date, I believe C.P. may share the residence with at least one other adult and a minor.

21. As outlined above, multiple sources of information indicate that C.P., currently resides at the SUBJECT PREMISES and resided there on the dates that child pornography files were uploaded from the SUBJECT IP ADDRESS. Though C.P. was the subscriber of the SUBJECT IP ADDRESS during the date(s) and time(s) of the uploads of child pornography, the more important factor is the physical location of the SUBJECT IP ADDRESSES at that time, which was the SUBJECT PREMISES. Based on my knowledge, training, and experience, and the experience of other law enforcement officers, I know that it is common for multiple individuals and computers within a residence to share Internet access. I believe that someone used at least one computer



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

from the SUBJECT PREMISES to distribute child pornography via the Internet, and that evidence of that crime will be found in the SUBJECT PREMISES.

## V. PRIOR EFFORTS TO OBTAIN EVIDENCE

22. Any other means of obtaining the necessary evidence to prove the elements of computer/Internet-related crimes, for example, a consent search, could result in an unacceptable risk of the loss/destruction of the evidence sought. If agents pursued a consent-based interview with C.P., or any other unknown resident(s) or occupant(s) of the SUBJECT PREMISES, they could rightfully refuse to give consent and the user who distributed child pornography files from a computer at the SUBJECT IP ADDRESS could arrange for destruction of all evidence of the crime before agents could return with a search warrant. Based on my knowledge, training and experience, the only effective means of collecting and preserving the required evidence in this case is through a search warrant. Based on my knowledge, no prior search warrant has been obtained to search the SUBJECT PREMISES.

## VI. TECHNICAL BACKGROUND

23. Based on my training and experience, when an individual communicates through the Internet, the individual leaves an IP address which identifies the individual user by account and ISP (as described above). When an individual is using the Internet, the individual's IP address is visible to administrators of websites they visit. Further, the individual's IP address is broadcast during most Internet file and information exchanges that occur.

24. Based on my training and experience, I know that most ISPs provide only one IP address for each residential subscription. I also know that individuals often use multiple digital devices within their home to access the Internet, including desktop and laptop computers, tablets, and mobile phones. A device called a router is used to connect multiple digital devices to the Internet via the public IP address assigned (to the subscriber) by the ISP. A wireless router performs the functions of a router but also includes the functions of a wireless access point, allowing (wireless equipped) digital



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

devices to connect to the Internet via radio waves, not cables. Based on my training and experience, today many residential Internet customers use a wireless router to create a computer network within their homes where users can simultaneously access the Internet (with the same public IP address) with multiple digital devices.

25. Based on my training and experience and information provided to me by computer forensic agents, I know that data can quickly and easily be transferred from one digital device to another digital device. Data can be transferred from computers or other digital devices to internal and/or external hard drives, tablets, mobile phones, and other mobile devices via a USB cable or other wired connection. Data can also be transferred between computers and digital devices by copying data to small, portable data storage devices including USB (often referred to as "thumb") drives, memory cards (Compact Flash, SD, microSD, etc.) and memory card readers, and optical discs (CDs/DVDs).

26. As outlined above, residential Internet users can simultaneously access the Internet in their homes with multiple digital devices. Also explained above is how data can quickly and easily be transferred from one digital device to another through the use of wired connections (hard drives, tablets, mobile phones, etc.) and portable storage devices (USB drives, memory cards, optical discs). Therefore, a user could access the Internet using their assigned public IP address, receive, transfer or download data, and then transfer that data to other digital devices which may or may not have been connected to the Internet during the date and time of the specified transaction.

27. Based on my training and experience, I have learned that the computer's ability to store images and videos in digital form makes the computer itself an ideal repository for child pornography. The size of hard drives used in computers (and other digital devices) has grown tremendously within the last several years. Hard drives with the capacity of four (4) terabytes (TB) are not uncommon. These drives can store thousands of images and videos at very high resolution.

28. Based on my training and experience, collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

services offered by companies such as Google, Yahoo, Apple, and Dropbox, among others. The online services allow a user to set up an account with a remote computing service that provides email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

29. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" and history files of the browser application used. A forensic examiner often can recover evidence suggesting whether a computer contains wireless software, and when certain files under investigation were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

30. Based on my training and experience, I have learned that producers of child pornography can produce image and video digital files from the average digital camera, mobile phone, or tablet. These files can then transferred from the mobile device to a computer or other digital device, using the various methods described above. The digital files can then be stored, manipulated, transferred, or printed directly from a computer or other digital device. Digital files can also be edited in ways similar to those by which a photograph may be altered; they can be lightened, darkened, cropped, or otherwise manipulated. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. In addition, there is an added



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

benefit to the child pornographer in that this method of production is a difficult trail for law enforcement to follow.

31. As part of my training and experience, I have become familiar with the structure of the Internet, and I know that connections between computers on the Internet routinely cross state and international borders, even when the computers communicating with each other are in the same state. Individuals and entities use the Internet to gain access to a wide variety of information; to send information to, and receive information from, other individuals; to conduct commercial transactions; and to communicate via email.

32. Based on my training and experience, I know that cellular mobile phones (often referred to as "smart phones") have the capability to access the Internet and store information, such as images and videos. As a result, an individual using a smart phone can send, receive, and store files, including child pornography, without accessing a personal computer or laptop. An individual using a smart phone can also easily connect the device to a computer or other digital device, via a USB or similar cable, and transfer data files from one digital device to another.

33. As set forth herein and in Attachment B to this Affidavit, I seek permission to search for and seize evidence, fruits, and instrumentalities of the above-referenced crimes that might be found at the SUBJECT PREMISES in whatever form they are found. It has been my experience that individuals involved in child pornography often prefer to store images of child pornography in electronic form. The ability to store images of child pornography in electronic form makes digital devices, examples of which are enumerated in Attachment B to this Affidavit, an ideal repository for child pornography because the images can be easily sent or received over the Internet. As a result, one form in which these items may be found is as electronic evidence stored on a digital device.

34. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

whom I have had discussions, I know that there are certain characteristics common to individuals who have a sexualized interest in children and depictions of children:

a. They may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. They may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, and/or drawings or other visual media. Such individuals often times use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts. These individuals may keep records, to include names, contact information, and/or dates of these interactions, of the children they have attempted to seduce, arouse, or with whom they have engaged in the desired sexual acts.

c. They often maintain any "hard copies" of child pornographic material that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain these "hard copies" of child pornographic material for many years, as they are highly valued.

d. Likewise, they often maintain their child pornography collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, often at the individual's residence or some otherwise easily accessible location, to enable the owner to view the collection, which is valued highly. They also may opt to store the contraband in cloud accounts. Cloud storage is a model of data storage where the digital data is stored in logical pools, the physical storage can span multiple servers, and often locations, and the physical environment is typically owned



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

and managed by a hosting company. Cloud storage allows the offender ready access to the material from any device that has an Internet connection, worldwide, while also attempting to obfuscate or limit the criminality of possession as the material is stored remotely and not on the offender's device.

e. They also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. They generally prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

g. E-mail itself provides a convenient means by which individuals can access a collection of child pornography from any computer, at any location with Internet access. Such individuals therefore do not need to physically carry their collections with them but rather can access them electronically. Furthermore, these collections can be stored on email "cloud" servers, which allow users to store a large amount of material at no cost, without leaving any physical evidence on the users' computer(s).

35. In addition to offenders who collect and store child pornography, law enforcement has encountered offenders who obtain child pornography from the internet, view the contents and subsequently delete the contraband, often after engaging in self-gratification. In light of technological advancements, increasing Internet speeds and worldwide availability of child sexual exploitative material, this phenomenon offers the offender a sense of decreasing risk of being identified and/or apprehended with quantities of contraband. This type of consumer is commonly referred to as a 'seek and delete' offender, knowing that the same or different contraband satisfying their interests remain easily discoverable and accessible online for future viewing and self-gratification. I



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

know that, regardless of whether a person discards or collects child pornography he/she accesses for purposes of viewing and sexual gratification, evidence of such activity is likely to be found on computers and related digital devices, including storage media, used by the person. This evidence may include the files themselves, logs of account access events, contact lists of others engaged in trafficking of child pornography, backup files, and other electronic artifacts that may be forensically recoverable.

36. Given the above-stated facts, including the circumstances surrounding the Google CyberTip and Rabbit user Lovr1's chats concerning the possible sexual abuse of minors, and based on my knowledge, training and experience, along with my discussions with other law enforcement officers who investigate child exploitation crimes, I believe that Rabbit user Lovr1 likely has a sexualized interest in children and depictions of children. I therefore believe that evidence of child pornography is likely to be found at the SUBJECT PREMISES.

37. Based on my training and experience, and that of computer forensic agents that I work and collaborate with on a daily basis, I know that every type and kind of information, data, record, sound or image can exist and be present as electronically stored information on any of a variety of computers, computer systems, digital devices, and other electronic storage media. I also know that electronic evidence can be moved easily from one digital device to another. As a result, I believe that electronic evidence may be stored on any digital device present at the SUBJECT PREMISES.

38. Based on my training and experience, and my consultation with computer forensic agents who are familiar with searches of computers, I know that in some cases the items set forth in Attachment B may take the form of files, documents, and other data that is user-generated and found on a digital device. In other cases, these items may take the form of other types of data - including in some cases data generated automatically by the devices themselves.

39. Based on my training and experience, and my consultation with computer forensic agents who are familiar with searches of computers, I believe that if digital



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

devices are found in the SUBJECT PREMISES, there is probable cause to believe that the items set forth in Attachment B will be stored in those digital devices for a number of reasons, including but not limited to the following:

a. Once created, electronically stored information (ESI) can be stored for years in very little space and at little or no cost. A great deal of ESI is created, and stored, moreover, even without a conscious act on the part of the device operator. For example, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache," without the knowledge of the device user. The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes affirmative steps to delete them. This ESI may include relevant and significant evidence regarding criminal activities, but also, and just as importantly, may include evidence of the identity of the device user, and when and how the device was used. Most often, some affirmative action is necessary to delete ESI. And even when such action has been deliberately taken, ESI can often be recovered, months or even years later, using forensic tools.

b. Wholly apart from data created directly (or indirectly) by user-generated files, digital devices - in particular, a computer's internal hard drive - contain electronic evidence of how a digital device has been used, what is has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating systems or application operations, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible for a user to use such specialized software to delete this type of information - and, the use of such special software may itself result in ESI that is relevant to the criminal investigation. HSI agents in this case have consulted on computer forensic matters with law enforcement officers with specialized knowledge and training in computers, networks, and Internet communications. In particular, to properly retrieve



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

and analyze electronically stored (computer) data, and to ensure accuracy and completeness of such data and to prevent loss of the data either from accidental or programmed destruction, it is necessary to conduct a forensic examination of the computers. To effect such accuracy and completeness, it may also be necessary to analyze not only data storage devices, but also peripheral devices which may be interdependent, the software to operate them, and related instruction manuals containing directions concerning operation of the computer and software.

## VII. SEARCH AND/OR SEIZURE OF DIGITAL DEVICES

40. In addition, based on my training and experience and that of computer forensic agents that I work and collaborate with on a daily basis, I know that in most cases it is impossible to successfully conduct a complete, accurate, and reliable search for electronic evidence stored on a digital device during the physical search of a search site for a number of reasons, including but not limited to the following:

a. Technical Requirements: Searching digital devices for criminal evidence is a highly technical process requiring specific expertise and a properly controlled environment. The vast array of digital hardware and software available requires even digital experts to specialize in particular systems and applications, so it is difficult to know before a search which expert is qualified to analyze the particular system(s) and electronic evidence found at a search site. As a result, it is not always possible to bring to the search site all of the necessary personnel, technical manuals, and specialized equipment to conduct a thorough search of every possible digital device/system present. In addition, electronic evidence search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since ESI is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code embedded in the system such as a "booby trap"), a controlled environment is often essential to ensure its complete and accurate analysis.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

b. Volume of Evidence: The volume of data stored on many digital devices is typically so large that it is impossible to search for criminal evidence in a reasonable period of time during the execution of the physical search of a search site. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Computer hard drives are now being sold for personal computers capable of storing up to four terabytes (4,000 gigabytes of data.) Additionally, this data may be stored in a variety of formats or may be encrypted (several new commercially available operating systems provide for automatic encryption of data upon shutdown of the computer).

c. Search Techniques: Searching the ESI for the items described in Attachment B may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant, and law enforcement personnel with appropriate expertise may need to conduct more extensive searches, such as scanning areas of the disk not allocated to listed files, or peruse every file briefly to determine whether it falls within the scope of the warrant.

41. In this particular case, and in order to protect the third party privacy of innocent individuals residing in the residence, the following are search techniques that will be applied:

i. Device use and ownership will be determined through interviews, if possible, and through the identification of user account(s), associated account names, and logons associated with the device. Determination of whether a password is used to lock a user's profile on the device(s) will assist in knowing who had access to the device or whether the password prevented access.

ii. Use of hash value library searches.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

iii. Use of keyword searches, i.e., utilizing key words that are known to be associated with the sharing of child pornography.

iv. Identification of non-default programs that are commonly known to be used for the exchange and viewing of child pornography, such as, eMule, uTorrent, BitTorrent, Ares, Shareaza, Gnutella, etc.

v. Looking for file names indicative of child pornography, such as, PTHC, PTSC, Lolita, 3yo, etc. and file names identified during the undercover download of child pornography.

vi. Viewing of image files and video files.

vii. As indicated above, the search will be limited to evidence of child pornography and will not include looking for personal documents and files that are unrelated to the crime.

42. These search techniques may not all be required or used in a particular order for the identification of digital devices containing items set forth in Attachment B to this Affidavit. However, these search techniques will be used systematically in an effort to protect the privacy of third parties. Use of these tools will allow for the quick identification of items authorized to be seized pursuant to Attachment B to this Affidavit, and will also assist in the early exclusion of digital devices and/or files which do not fall within the scope of items authorized to be seized pursuant to Attachment B to this Affidavit.

43. In accordance with the information in this Affidavit, law enforcement personnel will execute the search of digital devices seized pursuant to this warrant as follows:

a. Upon securing the search site, the search team will conduct an initial review of any digital devices/systems to determine whether the ESI contained therein can be searched and/or duplicated on site in a reasonable amount of time and without jeopardizing the ability to accurately preserve the data.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

b. If, based on their training and experience, and the resources available to them at the search site, the search team determines it is not practical to make an on-site search, or to make an on-site copy of the ESI within a reasonable amount of time and without jeopardizing the ability to accurately preserve the data, then the digital devices will be seized and transported to an appropriate law enforcement laboratory for review and to be forensically copied ("imaged"), as appropriate.

c. In order to examine the ESI in a forensically sound manner, law enforcement personnel with appropriate expertise will produce a complete forensic image, if possible and appropriate, of any digital device that is found to contain data or items that fall within the scope of Attachment B of this Affidavit. In addition, appropriately trained personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data fall within the list of items to be seized pursuant to the warrant. In order to search fully for the items identified in the warrant, law enforcement personnel, which may include investigative agents, may then examine all of the data contained in the forensic image/s and/or on the digital devices to view their precise contents and determine whether the data fall within the list of items to be seized pursuant to the warrant.

d. The search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to this Affidavit.

e. If, after conducting its examination, law enforcement personnel determine that any digital device is an instrumentality of the criminal offenses referenced above, the government may retain that device during the pendency of the case as necessary to, among other things, preserve the instrumentality evidence for trial, ensure the chain of custody, and litigate the issue of forfeiture.

44. In order to search for ESI that falls within the list of items to be seized pursuant to Attachment B to this Affidavit, law enforcement personnel will seize and



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

search the following items (heretofore and hereinafter referred to as "digital devices"), subject to the procedures set forth above:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any digital device used to facilitate the transmission, creation, display, encoding, or storage of data, including word processing equipment, modems, docking stations, monitors, printers, cameras, encryption devices, and optical scanners;

c. Any magnetic, electronic, or optical storage device capable of storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or memory buffers, smart cards, PC cards, memory sticks, flash drives, thumb drives, camera memory cards, media cards, electronic notebooks, and personal digital assistants;

d. Any documentation, operating logs and reference manuals regarding the operation of the digital device, or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the device hardware, or ESI to be searched;

f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the digital device, or ESI; and

g. Any passwords, password files, test keys, encryption codes or other information necessary to access the digital device or ESI.

//

//

//

//



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

## VIII. CONCLUSION

45. Based on the foregoing, I believe there is probable cause that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), are located at the SUBJECT PREMISES or on the SUBJECT PERSON as more fully described in Attachment A to this Affidavit, as well as on and in any digital devices found therein. I therefore request that the court issue a warrant authorizing a search of the location, vehicles, and person specified in Attachment A for the items more fully described in Attachment B.

Dated this 14th day of December, 2017.

Toby Ledgerwood, Affiant
Special Agent
Department of Homeland Security
Homeland Security Investigations

The above-named agent provided a sworn statement attesting to the truth of the contents of the foregoing affidavit on 14th day of December, 2017.

PAULA L. MCCANDLIS
United States Magistrate Judge



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

# ATTACHMENT A

## Description of Property to be Searched

The physical address of the SUBJECT PREMISES is 8575 Vinup Rd, Apt B, Lynden, Washington, and is more fully described as Unit B of the two-story, multi-unit residence with brown colored siding and white trim around the windows. The numbers 8575 are affixed in black lettering on the side of the building above the fire extinguisher. The letter "B" is in black located on a white door marking "Unit B." There are windows located on either side of the door to Unit B.

The search is to include all rooms and persons within the SUBJECT PREMISES, and all garages or storage rooms, attached or detached, or other outbuildings assigned to Unit B, and any digital device(s) found therein.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

**ATTACHMENT B**

**ITEMS TO BE SEIZED**

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed), photocopies or other photographic form, and electrical, electronic, and magnetic form (such as CDs, DVDs, smart cards, thumb drives, camera memory cards, electronic notebooks, or any other storage medium), that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) which may be found at the SUBJECT PREMISES:

1. Any visual depiction of minor(s) engaged in sexually explicit conduct, in any format or media.

2. Evidence of the installation and use of P2P software, and any associated logs, saved user names and passwords, shared files, and browsing history;

3. Letters, e-mail, text messages, and other correspondence identifying persons transmitting child pornography, or evidencing the transmission of child pornography, through interstate or foreign commerce, including by mail or by computer;

4. All invoices, purchase agreements, catalogs, canceled checks, money order receipts, credit card statements or other documents pertaining to the transportation or purchasing of images of minors engaged in sexually explicit conduct;

5. Any and all address books, names, lists of names, telephone numbers, and addresses of individuals engaged in the transfer, exchange, or sale of child pornography;

6. Any non-digital recording devices and non-digital media capable of storing images and videos.

7. Digital devices and/or their components, which include, but are not limited to:

a. Any digital devices and storage device capable of being used to commit, further, or store evidence of the offense listed above;



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

b. Any digital devices used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, cameras, printers, encryption devices, and optical scanners;

c. Any magnetic, electronic, or optical storage device capable of storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or memory buffers, smart cards, PC cards, memory sticks, flashdrives, USB/thumb drives, camera memory cards, media cards, electronic notebooks, and personal digital assistants;

d. Any documentation, operating logs and reference manuals regarding the operation of the digital device or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

g. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data;

8. Evidence of who used, owned or controlled any seized digital device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, saved user names and passwords, documents, and browsing history;

9. Evidence of malware that would allow others to control any seized digital device(s) such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malware; as well as evidence of the lack of such malware;

10. Evidence of the attachment to the digital device(s) of other storage devices or similar containers for electronic evidence;

11. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from a digital device;



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

12. Evidence of times the digital device(s) was used;

13. Any other ESI from the digital device(s) necessary to understand how the digital device was used, the purpose of its use, who used it, and when.

14. Records and things evidencing the use of the IP address 73.53.83.83 (the SUBJECT IP ADDRESS) including:

a. Routers, modems, and network equipment used to connect computers to the Internet;

b. Records of Internet Protocol (IP) addresses used;

c. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

**The seizure of digital devices and/or their components as set forth herein is specifically authorized by this search warrant, not only to the extent that such digital devices constitute instrumentalities of the criminal activity described above, but also for the purpose of the conducting off-site examinations of their contents for evidence, instrumentalities, or fruits of the aforementioned crimes.**



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970